NASA COOPERATIVE AGREEMENT

NCC 2-609

FINAL TECHNICAL REPORT

Principal Investigator: Dr. William Dunn, Jr.

Period Covered by Report: October 1, 1988 through September 30, 1995

Institution: University of Southern Colorado
2200 Bonforte Blvd.
Pueblo, Colorado 81001

Technical Officer: Laura Doty

CONTENTS

NASA COOPERATIVE AGREEMENT

NCC 2-609

FINAL TECHNICAL REPORT

1.0 General Summary

Work during the course of the above agreement resulted in five open-literature publications. Cumulated references to these publications follows this general summary.

Research under Cooperative Agreement NCC 2-609 was prompted by what were perceived to be shortcomings in SR&QA practice on aeronautical, facility, and space projects not only at Ames but elsewhere in government and industry.

Foremost, SR&QA resources were (accurately) seen at that time to be dwindling. The luxury of having a cadre of safety analysts, reliability experts, and quality assurance specialists available to work with an SR&QA analyst on a given project was fast disappearing. It would therefore be necessary to cut deeply into the fat and integrate the combined talents of these individuals into a single unified activity which could be performed by a single analyst - yet provide the same quality level of safety and mission risk assessment.

Complicating the effect of diminishing resources and a pressing need to "do more for less" was the fact that systems were being built with new implementation technologies notably in digital control, data communications, and software - technologies lying well beyond SR&QA experience of Ames at the time. It would be necessary to find highly efficient methods for assessing these new complex technologies and integrating these methods into the new single activity.

As elsewhere, SR&QA assessment efforts and recommendations tended to appear quite late in the design cycle where changes based on the recommendations bore high cost. To optimize cost effectiveness of risk assessment it became imperative that the new activity should not only be done early in the design cycle but that it should drive, and not simply chronicle, system design.

Finally, it was believed that quantitative measures of reliability and safety should be incorporated, where needed, to guide risk decision making.

As an initial step quantitative methods for risk assessment of digital control hardware and software systems were investigated at Ames for applicability to facility, aeronautical and space systems. At the time, NASA Headquarters was investigating the use of probabilistic

risk assessment (PRA) techniques as practiced in the nuclear industry. In 1990, NASA Headquarters funded a three-day workshop on PRA held at Ames. The workshop was followed up in 1991 by six-month course in PRA given also at Ames. Over the remaining years of the grant , USC and Ames researchers took up the challenge of simplifying the locally-developed digital hardware and software methods and condensing the highly sophisticated PRA techniques into a simplified yet highly effective approach for both safety and mission risk assessment of facility, aeronautical, and space systems.

The overall approach was given the name Integrated Risk Assessment (IRA). The approach was tested and refined by applying it to actual facility, aeronautical, and space applications at Ames.

Technical details of the IRA approach and application to actual examples are presented in Reference 1. [References 2 through 4 were also supported in part by the Cooperative Agreement.]

2.0 Cumulated References

The following references were supported in whole or part by the Agreement.

1. Dunn, W.R.: Integrated Risk Assessment Handbook to be published by NASA Ames Research Center.

2. Dunn, W.R.; Doty, L.W.; Frank, M.V.; and Epstein, S.A.: Risk Assessment and Management of Safety-Critical, Digital Industrial Controls - Present Practices and Future Challenges. PSAM II Conference, San Diego CA, March 20-24, 1994.

3. Carroll, C.; Dunn, W.; Doty, L.; Frank, M.; and Hulet, M.: Reliability-Based Design of a Safety-Critical Automation System - A Case Study. PSAM II, San Diego CA, March 20-24, 1994.

4. W. Dunn; R. Folsom; and O. Green: Latent-Failure Risk Estimates for Computer Control. Reliability and Maintainability Symposium, Orlando FL, January 29-31, 1991.

5. Dunn, W. and Corliss, L.: Software Safety: A User's Practical Perspective. Reliability and Maintainability Symposium, Los Angeles, CA, January 23-25, 1990.